

This is a combined synopsis/solicitation for commercial services prepared in accordance with the format in FAR 12.6 and FAR Part 13, as supplemented with additional information included in this notice. The incorporated provisions and clauses are those in effect through Federal Acquisition Circular (FAC) 2005-89.

THIS ANNOUNCEMENT CONSTITUTES THE ONLY SOLICITATION AND A SEPARATE SOLICITATION WILL NOT BE ISSUED. The solicitation number for this acquisition is ED-FSA-R-16-000729. The NAICS Code for this solicitation is 517210. This will be awarded as a 100% Total Small Business Set-Aside . Prospective Offerors are responsible for downloading the solicitation and any amendments. It is the Offeror's responsibility to monitor the FBO website for the release of any amendments to this solicitation. The Government reserves the right to award a purchase order without discussions if the Contracting Officer determines that the initial offer(s) is/are providing the Best Value and discussions.

The solicitation is being issued as a Request for Quote (RFQ).

This will be a Fixed Priced Purchase Order.

The Department of Education, Federal Student Aid (FSA), Information Technology Office has a need to integrate Outbound Short Message Service (SMS) as an alternate method of communication within Person Authentication System (PAS).

#### **A. BACKGROUND AND OVERVIEW:**

Federal Student Aid (FSA) is using the Person Authentication System (PAS), to allow FSA's non-privileged users (aid applicants, students, parents, borrowers, and others) to securely access FSA Systems and data. PAS will allow users to create, manage, and login to publicly available FSA systems, such as FAFSA, NSLDS and Student Loans using PAS accounts. PAS has a requirement to support 80 million user accounts, 100 thousand concurrent sessions, 80 authentications per second, 220 million authentications per year, supporting a growth rate of 10 percent a year.

PAS currently communicates with its user base through email. FSA would like to integrate Outbound Short Message Service (SMS) as an alternate method of communication within PAS.

#### **B. OBJECTIVES/PURPOSE**

FSA has a need to integrate Outbound Short Message Service (SMS) as an alternate method of communication within PAS. PAS developers would communicate with the SMS Contractor via API calls. The SMS messages would be used to inform the user of PAS related events such as account creation or successful password recovery. These events are time limited, so the message would need to meet the time requirements of PAS.

PAS would send a SMS Message for each of the following events:

Name	Description	Type
Create Account	PAS Account is created	Real Time
Account Locked	User selects to use e-mail for self-service	Real Time
Forgot Password	User needs to recovery password via self-service	Real Time
Forgot Username	User needs to recovery userid via self-service	Real Time
Resend secure code SMS	User selects to resend secure code	Real Time
Account Change	Updates are made to user account by user or admin	Real Time
Password Change	Password is changed	Real Time
Account Disabled	Status Change - Account Disabled	Real Time
Account Enabled	Status Change - Account Enabled	Real Time
Account Locked	Status Change - Account Locked – 3rd attempt	Real Time

### C. PRICING SCHEDULE

SMS Text Costs Annual Estimate	Price/per SMS	SMS/Month	Price/Month	Emails / Month	Total
Base Period	\$	\$ /8,300,000	\$	Not-to-Exceed 49,800,000	\$
Option Period 1	\$	\$ /8,333,333	\$	Not-to-Exceed 99,999,996	\$
Option Period 2	\$	\$ /8,333,333	\$	Not-to-Exceed 99,999,996	\$
Option Period 3	\$	\$ /8,333,333	\$	Not-to-Exceed 99,999,996	\$

Option Period 4	\$	\$ /8,333,333	\$	Not-to-Exceed 99,999,996	
<b>Total</b>					

\*\*\*\*\*The pricing schedule shall be for a six (6) month Base Period and 4 one year Option Periods include dashboard metrics capability along with including the Carrier tariffs in quoted price

**D. PLACE OF PERFORMANCE and INSPECTION/ACCEPTANCE:**

FOB: DESTINATION

Department of Education, Federal Student Aid (FSA)  
Union Center Plaza (UCP)  
830 First Street, NW  
Washington DC 20202

**E. PERIOD OF PERFORMANCE**

Base Period: August 22, 2016 through February 21, 2017  
Option Period 1: February 22, 2017 through February 21, 2018  
Option Period 2: February 22, 2018 through February 21, 2019  
Option Period 3: February 22, 2019 through February 21, 2020  
Option Period 4: February 22, 2020 through February 21, 2021

**F. STATEMENT OF OBJECTIVE (SOO)**

*Requirements:*

**F.1 The SMS system shall perform the following functions:**

1. Receive real-time requests from the PAS system for individual SMS Text messages with the expected delivery time to the end user not to exceed 1 minute. This is required to support time-critical user transactions.
2. Support templates for predefined SMS formats, so that only the variable part of the content needs to be provided to compose SMS Text messages.

**F.2 The SMS system shall have the following capabilities:**

1. Provide system availability of 99.999%.
2. Provide a successful delivery rate to carrier that meet or exceed 99.999%.
3. Provide monthly metrics that can verify delivery percentage of 99.999%.
4. Support up to 100 million SMS Text messages per year.
5. Support a peak SMS send rate of up to 50 per second.
6. Adjust capacity to reflect varying monthly peak usage, with peak day volume of up to 1 million SMS Text messages.
7. Provide compliance to federal standards such as CAN-SPAM and TCPA.
8. Retain an audit trail of SMS Text messages sent (addressee, content, unsuccessful attempts) for a minimum of 30 days.
9. All servers and datacenters that support the SMS service are located within the United States.
10. All helpdesk, server administrators and other personal that support the SMS service reside within the United States.
11. Provide flexible customer support options. Provide dedicated service manager and customer service responsiveness within 1 hour.

**F.3 The SMS service provider shall provide the following services:**

1. Provide and manage opt in, opt out and messaging permissions.
2. Provide 24x7 telephone/online chat support for escalation of issues.
3. Use industry best practices to ensure that SMS Text source will not be perceived by recipients' carriers as spam and prevented from reaching the recipient.
4. Ensure that high volumes of SMS Text messages will not be perceived by recipients' carriers as spam and prevented from reaching the recipient, or place the originator on industry black lists.
5. Ensure that SMS Text message content and format will not be perceived by recipients' carriers as spam and prevented from reaching the recipient, or place the originator on industry black lists.
6. Provide the following analytics on a monthly basis (The first 2 months shall require daily reporting)
  - a. SMS Delivery Metrics (Successful, Failed, Bounced messages)
  - b. # of SMS Text messages sent out during a month
  - c. Average delivery time for SMS text messages
7. Provide and manage the appropriate short code(s) needed to source the SMS messages.
8. Provide a callback ability that if enabled would allow the PAS system to receive SMS delivery status from the SMS provider.

**G. DELIVERABLES:**

1. Provide daily metric report for First two months.
2. Provide monthly metric report for SMS service.

**H. EVALUATION AND AWARD:**

52.212-1 Instructions to Offerors—Commercial Items. (FEB 2012)

52.212-3 Offeror Representations and Certifications—Commercial Items. (APR 2012)

Award. The Government intends to evaluate proposals and, if necessary conduct discussions. The award will be made to the Offeror whose proposal conforms to the terms and conditions of the solicitation and award may be made to other than the lowest priced or the highest technically rated offer.

Relative importance and trade-offs. The Government will base the determination of best value on performance, and the other evaluation factors identified elsewhere in this solicitation. The determination of best value also considers the relative importance of the evaluation factors. Technical factors and past performance when combined are significantly more important than price. It is pointed out, however, should technical competence between Offerors be considered approximately the same, then price could become primary.

FSA will base its award decision using a best value analysis that results in the most advantageous acquisition for the Government. FSA's acquisition strategy used to obtain best value may result in an award to other than the lowest priced, technically rated Offeror. Best value analysis spans a continuum from the lowest priced, technically acceptable proposal to those proposals in which tradeoffs between price, past performance, and each Offeror's technical solution is evaluated.

52.212-2 Evaluation—Commercial Items. (JAN 1999)

(a) The Government will award a purchase order resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors (equally weighted 1-4) shall be used to evaluate offers:

1. Capacity/Throughput
2. Customer Support
3. Reporting/Tracking
4. Client Base
5. Price

Technical factors and past performance when combined are significantly more important than price.

(b) *Options*. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

The total number of pages for the technical proposal shall not exceed fifteen (15) pages, using 1" margins, single spaced, font type Time New Roman, and a font size of 12.

*\*Proposals shall be in 2 volumes: 1 Technical and 1 Price. The volumes shall be separate and complete, so that evaluation of one may be accomplished independently of, and concurrently with, the evaluation of the other. No pricing information shall be provided in the Technical volume.*

**\*\***The solicitation does not commit the Government to pay any cost for the preparation and submission of a quote or proposal. It is also advised that the Contracting Officer (CO) is the only individual who can legally commit and obligate the Government to the expenditure of public funds in connection with the proposed acquisition.

SAM: Vendors must be registered and active in the System for Award Management (SAM) prior to the award of a contract. You may register by going to [www.sam.gov](http://www.sam.gov). You will need your Dun & Bradstreet number and banking information.

**QUESTIONS DEADLINE:** All question requests for FSA are to be submitted via email to [FSAEAT@ed.gov](mailto:FSAEAT@ed.gov) no later than August 10, 2016 1:00pm EST. Be sure to reference solicitation number: Questions/ED-FSA-R-16-000729 and your company name in the subject line.

**QUOTATIONS DUE:** All quotations are due via email to: [FSAEAT@ed.gov](mailto:FSAEAT@ed.gov) no later than 1:00pm, EST on August 16, 2016. Be sure to reference solicitation number: ED-FSA-R-16-000729 and your company name in the subject line.

## **DEPARTMENT OF EDUCATION CLAUSES**

### **3452.201-70 Contracting Officer's Representative (COR) (MAR 2011)**

(a) The Contracting Officer's Representative (COR) is responsible for the technical aspects of the project, technical liaison with the Contractor, and any other responsibilities that are specified in the contract. These responsibilities include inspecting all deliverables, including reports, and recommending acceptance or rejection to the contracting Officer.

(b) The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes that affect the contract price, terms, or conditions. Any Contractor requests for changes shall be submitted in writing directly to the Contracting Officer or through the COR. No such changes shall be made without the written authorization of the Contracting Officer.

(c) The COR's name and contact information:

Name: *Name and Contact information to be determined upon award*  
Address: Department of Education  
Federal Student Aid  
830 First Street, NE  
Washington, DC 20202  
Email:  
Tel No:

(a) The COR may be changed by the Government at any time, but notification of the change, including the name and address of the successor COR, will be provided to the Contractor by the Contracting Officer in writing.

#### **3452.239-70 Internet protocol version 6 (IPv6)(MAR 2011)**

(a) Any system hardware, software, firmware, or networked component (voice, video, or data) developed, procured, or acquired in support or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet protocol (IP) version 6 (IPv6) as set forth in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2460 and associated IPv6-related IETF RFC standards. In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability capabilities of IPv4 products.

(b) Specifically, any new IP product or system developed, acquired, or produced must—

(1) Interoperate with both IPv6 and IPv4 systems and products; and

(2) Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

(c) Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval.

#### **3452.239-71 Notice to offerors of Department security requirements (MAR 2011)**

(a) The offeror and any of its future subcontractors will have to comply with Department security policy requirements as set forth in the "Bidder's Security Package: Security Requirements for Contractors Doing Business with the Department of Education" at:

<http://www.ed.gov/fund/contract/about/bsp.html>.

(b) All contractor employees must undergo personnel security screening if they will be employed for 30 days or more, in accordance with Departmental Directive OM:5-101, "Contractor Employee Personnel Security Screenings," available at:

<http://www.ed.gov/fund/contract/about/acs/acsom5101.doc>.

(c) The offeror shall indicate the following employee positions it anticipates to employ in performance of this contract and their proposed risk levels based on the guidance provided in Appendix I of Departmental Directive OM:5-101:

High Risk (HR): [Specify HR positions.].

Moderate Risk (MR): (5C) Program Manager and other labor categories identified in the award.

Low Risk (LR): [Specify LR positions.].

(d) In the event the Department disagrees with a proposed risk level assignment, the issue shall be subject to negotiation. However, if no agreement is reached, the Department's risk level assignment shall be used. The type of screening and the timing of the screening will depend upon the nature of the contractor position, the type of data to be accessed, and the type of information technology (IT) system access required. Personnel security screenings will be commensurate with the risk and magnitude of harm the individual could cause.

## **FSA CLAUSES**

### **FSA 32-1 INVOICE PROCEDURES (MAR 2012)**

The Contractor must submit an invoice via mail, fax, or e-mail for this contract in order to be paid for products and/or services rendered. For Prompt Payment Act purposes, Invoices received after 3 p.m. will be processed on the next business day.

Federal Student Aid's "Designated Billing Office" (DBO) is:

US Department of Education  
Union Center Plaza  
Federal Student Aid Administration  
830 First Street, NE – Suite 54B1  
Washington, D.C. 20201-0001  
E-mail: [Invoice.Admin@ed.gov](mailto:Invoice.Admin@ed.gov)  
Fax: (202) 275-3477

A Contractor shall also simultaneously submit copies of the invoice to the Contracting Officer

(CO) and one to the Contracting Officer's Representative (COR). The CO and COR should receive copies via the same means as the invoice sent to the DBO.

When submitting an invoice via mail, the Contractor shall submit the original invoice and two copies of the invoice.

At a minimum, the following items must be addressed in order for the invoice to be considered “proper” for payment:

- (1) Name and Address of the Contractor.
- (2) Invoice Number and Invoice Date.
- (3) The Contract number, contract line item, and if applicable, the order number.
- (4) Description, quantity, unit of measure, unit price, and extended price of the delivered item or service, as defined in the contract or order.
- (5) Terms of any offered prompt payment discount.
- (6) Name, title, and phone number of persons to be notified in event of a defective invoice.
- (7) The period of time covered by the invoice.
- (8) Totals, supported by subtotals, and subtotals should be supported by detail (i.e. documentation for categories of labor, hours performed, unit prices) and deliverables provided.
- (9) If required by this contract or order, receipts must be provided to support documentation of “other direct costs” (ODCs) or materials.
- (10) Special instructions for finance payments:  
Invoices for finance payments shall specifically and prominently identify the payment request as follows:

#### REQUEST FOR FINANCING PAYMENT

Finance payments are not subject to the Prompt Payment Act. Failure to identify the invoice as a request for financing may result in delay of payment. Invoices that are identified as Requests for Finance Payments shall only include the finance payments listed in the contract. Requests for finance payments shall not be combined with other types of invoice payments.

#### **FSA 37-3 DISRUPTION OF MISSION CRITICAL CONTRACTOR SYSTEM OR OTHER SERVICES (SEP 2012)**

(a) Definition. As used in this clause—

- (1) Mission Critical Contractor System or Other Services - are defined as a system or other services that have a material impact on the accomplishment of the Federal Student Aid mission.
- (b) The Contractor is required to coordinate all changes to mission critical Contractor systems or other services used to implement Federal Student Aid IT operations and services with the individual(s) identified in (c) at least five business days prior to the changes, absent exigent circumstances. Emergency changes require immediate notification of the individual(s) identified in (c) as soon as the change requirement is known, but prior to the change. If the continuity of such systems or services is disrupted as a consequence of the Contractor’s failure to adequately coordinate these changes with FSA, the Contractor may be subject to contractual remedies

available to the government pursuant to the terms of the contract or as authorized by law.

(c) The Contractor shall contact the following individuals to coordinate all changes to mission critical Contractor systems or services.

(To Be Determined)

## **FSA 45-1 SPECIAL CONTRACT REQUIREMENTS FOR GOVERNMENT FURNISHED PROPERTY – TWO FACTOR AUTHENTICATION TOKENS (TFA) (JUN 2015)**

In addition to the requirements of FAR 52.245-1(b) - Government Property, the Contractor shall:

- a) Ensure the Contractor's Government Property Manager or designee shall sign a distribution letter provide by the Contracting Officer upon receipt of Government Property;
- b) Comply with instructions on how to register the tokens using the Federal Student Aid Two Factor Authentication Token For FSA User Handout distributed with the tokens;
- c) Seek immediate assistance with any challenges encountered with FSA CITRIX and TFA and immediately report any security or other incidents by telephone or email to the helpdesk at: 1-877-603-4188 or [ed.customer.service@ed.gov](mailto:ed.customer.service@ed.gov) and;
- d) Provide a Property Management Plan to the Contracting Officer within 5 business days of receipt of the Government Furnished Property. Among other requirement required under FAR 52.245-1(b) the Property Management Plan must contain at minimum the following:
  - Description on how the Contractor shall establish and maintain an auditable record of the token assignment to its employees by individual name and token Serial Number (AVT+9 digits);
  - Method by which the Contractor shall ensure that the serial number label on the back of each token remains legible and secure to the device.
  - Security and management process for the physical devices as well as changes in assignment.
- e) Upon written notification from the Contracting Officer, the Contractor shall affirm its understanding and compliance with the Government's requirement for quarterly re-certification of user access and token activation. In the event of any reported security breach, the Government shall immediately disable or deactivate Contractor access to its network without prior notice.
- f) Soft Tokens can be used instead of hard tokens. The soft token is an app that runs on the user's mobile device. After downloading and registering the free Symantec VIP Access app on a phone or tablet, a user simply opens the app and an One-Time Password (OTP) is automatically generated similar to a hard token. Use of a soft token is optional, however users who have a compatible mobile device are encouraged to transition to a soft token. There is no requirement to maintain property records on soft tokens.

- g) **Contact Information.** For additional information on TFA or the use of a soft token, contact the TFA Support Center at 800/330-5947, option 2 (TDD/TTY 800/511-5806) or by email at [TFASupport@ed.gov](mailto:TFASupport@ed.gov).

### FSA Service Level Agreements for Contractor Employee Clearance Monitoring

SLA #	Objective	Measurement	Standard/Period (w/disincentive (if applicable))	Notes
1	Timely e-Qip submission. Submit e-Qip form to the COR/ISSO within 24 hours of a contractor employee's assignment to a Department contract and ensure that the forms are accurate and complete (reference EDARS 3452.239-72). (Time frame may change based upon Departmental policy)	Send a confirmation email to the FSA CO/COR/ISSO and Program Management by 5:00PM of the due date that certifies the success of complete, accurate, and timely clearance submission	95% complete, accurate, and timely submissions over monthly period  Period – Monthly Metric  Disincentive - \$5,000 per 6C, \$2,500 per 5C, and \$500 per 1C over the standard in the reporting period	Example: For a contractor employee reporting for duty Monday, August 17, 2015, e-Qip initiation form must be received by 5:00PM of Tuesday, August 18, 2015.
2	Timely resolution of e-Qip information deficiencies. If any information on forms required by e-Qip are not complete or the submission is returned for any reason, the contractor must resubmit the forms to the COR/ISSO within 7 (reference OM: 5-101) business days or the contractor employee must be removed from the contract	Send a confirmation email to the FSA CO/COR/ISSO and Program Management by 5:00PM of the due date that certifies the success of timely clearance form re-submission or the removal of the contract employee from the contract	99% complete, accurate, and timely re-submission over monthly period  Period – Monthly Metric  Disincentive - \$5,000 per 6C, \$2,500 per 5C, and \$500 per 1C over the standard in the reporting period	
3	Clearance Monitoring - When clearance information is returned with clearance type and date issued, monitor contractor employee clearance	A consolidated report of all employees in the format shown below will be submitted to the COR and ISSO (copy to the CO) within 5 business	95% complete and accurate over quarterly period	Submittal of quarterly report does not replace timely requests for e-Qip for new employees, monitoring status of clearance/clearance

	and employment status under the contract to ensure clearances renewals are submitted 30 calendar days prior to expiration, departed employees are identified and removed, and any clearance changes are annotated.	days following each three month period of performance for identification of changes over the last quarter (new employees, employees with clearance in process (and status), change in clearance type, and resubmittals for employees 30 calendar days prior to clearance expiration and departed employees).	Period – Quarterly Metric  Disincentive - \$1,000 per error over the standard in the reporting period	renewal requests, requesting clearance renewals 30 days before expiration, or notification that an employee has departed. COR will spot check quarterly and submit annually to the Security Office for a 100% validation when requested.
4	Timely Submittal of Clearance Renewals. EDARS 3452.239-72 requires contractor employees in High Risk 6 (C) positions to submit clearance packages for re-investigation every five years. Once a contractor employee receives their clearance, an issuance and expiration date will be provided back to the contractor for tracking. Contractors must submit re-investigation packages to e-Qip 30 calendar days prior to clearance expiration.	A confirmation email to the FSA CO/COR/ISSO and Program Management 30 calendar days prior to the Clearance expiration date that certifies the success of complete, accurate, and timely clearance re-submissions.	95% complete, accurate, and timely submission over quarter  Period – Quarterly Metric Disincentive - \$1,000 per error over the standard in the reporting period	

Contractor/Subcontractor	Contract Number	Employee Last Name	Employee First Name	Employee Middle Name (if known)	Job Title (indicate if supervisory)	Employee Status (fulltime, part time, temporary, surge, etc.)	System(s) Access	Normalized System Name	ISSO	CO	COR
--------------------------	-----------------	--------------------	---------------------	---------------------------------	-------------------------------------	---	------------------	------------------------	------	----	-----

## **PIV Card Implementation to Access FSA Data for Privilege Users (September 2015)**

### **I. BACKGROUND.**

To improve the Federal cybersecurity and protect IT systems against threats, FSA is tightening policies and practices for Privilege Users by:

- a) Implementing multi-factor authentication for Privilege Users through PIV cards.
- b) Minimizing the number of Privilege Users, limiting the login duration, limiting functions they can perform while logged in, and ensuring that all activities are logged and reviewed regularly.

### **II. DEFINITIONS.**

- a) A Privilege User is defined as a user of an Information System with more authority and access than a general user (for example: users with root access, Database Administrators, Application Administrators, Network Administrator, System Administrator, Information Assurance Manager/Information Assurance Officer).
- b) A PIV Card is an identity card that is issued by the Federal Government and is fully compliant with Federal PIV standards (e.g., Federal Information Processing Standard (FIPS) 201).
- c) A PIV Interoperable Card (PIV-I) is an identity card that meets the PIV technical specifications to work with PIV infrastructure elements, such as card readers, and is issued in a manner that allows Federal Government relying parties to trust the card. PIV-I Non-Federally Issued (NFI) identity cards must conform to the NIST technical specifications for a PIV Card as defined in NIST SP 800-73 and meet the cryptographic requirements of FIPS 140 and NIST SP 800-78. Please refer to the “Personal Identity Verification Interoperability For Non-Federal Issuers” document at <http://www.idmanagement.gov/personal-identity-verification-interoperability>.
- d) A Card Reader is a device which complies with the requirements as specified in NIST SP800-96 and conforms to the ISO7816 standard for the card-to-reader interface. These readers also conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface in general desktop computing environment.

### **III. REQUIREMENTS.**

- a.) No later than 5 working days from date of contract award, provide the cognizant Contracting Officer the following:

- The total number of Privilege Users

- The firm, either Contractor or Subcontractor, the Privilege User works for
- Each Privilege User's location
- Full name of each Privilege User
- Each Privilege User's role
- The IT resource(s) and application(s) containing or accessing FSA's data Resource(s) being accessed by each Privilege User
- Current method of accessing the IT resource(s) and application(s) containing or accessing FSA's data
- Identify each Privilege User which already has a PIV card (if applicable)
- Identify each Privilege User which already has a Two-Factor token, if applicable)
- Identify each Privilege User that already has a VPN account (if applicable)
- 

b.) Government Furnished Property and Systems Solutions

- 1) FSA will issue and distribute all PIV cards for all Privilege users accessing the Virtual Data Center (VDC) (or its successor) resources.
- 2) FSA has implemented the CyberArk Privilege Account Security (CPAS) solution for VDC (or its successor) to protect the Privilege accounts from misuse and provide assurance that such accounts are controlled and managed. Implementation of the CPAS solution:
  - Limits functions that can be performed when using Privilege accounts
  - Limits the duration that Privilege Users can be logged in
  - Ensures that all Privilege User activities are logged

c.) *(The following applies if the contractor has 25 or fewer employees performing duties as Privilege User at the place of performance; AND the place of performance is located within 2.5 hours of the Department of Education Headquarters or listed Regional Office locations (see attached) by motor vehicle.*

The contractor shall ensure all contractor employees identified as Privilege Users travel to the Department of Education Headquarters or listed Regional Office locations (see attached) to receive the FSA issued PIV Card.

d.) *(The following applies if the contractor has a number of Privilege Users in a place of performance exceeds 25 persons, or the place of performance exceeds a 2.5-hour trip by motor vehicle.)*

The contractor shall ensure all contractor employees identified as Privilege Users are available to travel to a FSA identified location to receive the FSA issued PIV Card.

- e.) Once the PIV Cards are issued, the contractor shall ensure that all Privilege Users who work on IT resources and applications containing or accessing FSA's data shall utilize PIV cards.
- f.) The contractor's Privilege Users shall access FSA's Virtual Data Center (VDC) (or its successor) resource through VPN.
- g.) Note: FSA **will not** provide a PIV Card Reader. The contractor shall provide compliant PIV card readers to each Privilege User.
- h.) The contractor's Privilege Users shall login through the CyberArk login portal using the PIV Card through the contractor provided PIV Card Reader.
- i.) The contractor's Privilege Users shall select the entitled resources (server, mainframe, networking equipment) retrieved by CyberArk's Role Based Access Control (RBAC) authentication.
- j.) Additional login instructions for accessing CyberArk portal through the VPN tunnel are attached.

**Attachment: Examples of Privilege User Roles and Job Functions (All Environments)**

**Database Administrator:**

- Installing and upgrading the database server and application tools
- Allocating system storage and planning future storage requirements for the database system
- Modifying the database schema, as necessary, from information given by application developers
- Enrolling users and maintaining system security
- Controlling and monitoring user access to the database
- Monitoring and optimizing the performance of the database
- Maintaining archived data
- Backing up and restoring databases

**Application Administrator:**

- Perform application tuning, configuration, monitoring, and administration.
- Plan and manage application software upgrades.
- Analyze custom administrative software requests and present solutions.
- Optimize application performance.
- Perform daily monitoring and capacity planning for enterprise information systems.

**System Administrator:**

- Analyzing system logs and identifying potential issues with computer systems.
- Introducing and integrating new technologies into existing data center environments.
- Performing routine audit of systems and software.

- Applying operating system updates, patches, and configuration changes.
- Installing and configuring new hardware and software.
- Adding, removing, or updating user account information, resetting passwords, etc.
- Responsible for documenting the configuration of the system.
- Troubleshooting any reported problems.
- System performance tuning.
- Ensuring that the network infrastructure is up and running.
- Configuring, adding, and deleting file systems.

### **Network Administrator:**

- Install and support LANs, WANs, network segments, Internet, and intranet systems.
- Install and maintain network hardware and software.
- Analyze and isolate issues.
- Monitor networks to ensure security and availability to specific users.
- Evaluate and modify system's performance.
- Maintain integrity of the network, server deployment, and security.
- Deploy networks and network equipment.
- Perform network address assignment.
- Enter routing protocols and routing table configuration.
- Enter configuration of authentication and authorization of directory services.
- Maintain network servers such as file servers, VPN gateways, intrusion detection systems.
- Administer servers, desktop computers, printers, routers, switches, firewalls, phones, personal digital assistants, smartphones, software deployment, security updates and patches.

### **Information Assurance Manager/Officer:**

- Perform security tool administration providing risk analysis of the following:
  - Vulnerability scanners
  - Security event logging & monitoring analyzers
  - Intrusion Detection/Prevention System (IDS/IPS) and firewall logs
  - Performs system and network security audits
  - Anti-virus products and central console
- Perform the day to day operations, management and administration to protect the integrity, confidentiality, and availability of information assets and technology infrastructures of the organization:
  - IDS/IPS/Firewalls
  - Anti-virus
  - Event log analysis
  - Access the system or infrastructure to perform threat, vulnerability, and risk assessments
  - Access the system or infrastructure to manage/perform security audits
  - Access the system or infrastructure to perform or assist with investigations
  - Access the system or infrastructure to coordinates the handling and resolution of

incidents of security breach

- Day-to-day operations and maintenance of computer facilities and IT resources including network support, server support, desk top support, and telecommunications services.

**Attachment: Mandatory Use of PIV Cards upon request**

**Attachment: CyberArk Testing Procedures upon request**

PROVISIONS and CLAUSES: The provision at FAR 52.212-1, Instructions to Offerors Commercial Items applies to this solicitation. The following agenda has been attached to this provision: see above. Offerors shall include a completed copy of the provision at FAR 52.212-3, Offeror Representations and Certifications Commercial Items. The clause at FAR 52.212-4, Contract Terms and Conditions, Commercial Items applies to this acquisition. The following agenda has been attached to the clause: None. The clause at FAR 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders, Commercial Items applies to this acquisition. The following FAR clauses cited are applicable: FAR 52.203-13, FAR 52.209-6, FAR 52.217-5, FAR 52.217-8, FAR 52.219-6, FAR 52.219-8, FAR 52.219-28, FAR 52.222-3, FAR 52.222-19, FAR 52.222-21, FAR 52.222-56, FAR 52.222-35, FAR 52.222-36, FAR 52.222-37, FAR 52.223-15, FAR 52.223-18, FAR 52.225-1 and FAR 52.232-33, FAR 52.246-16. Clauses and provisions are incorporated by reference and apply to this acquisition.

No phone calls will be accepted.